Crowe Horwath

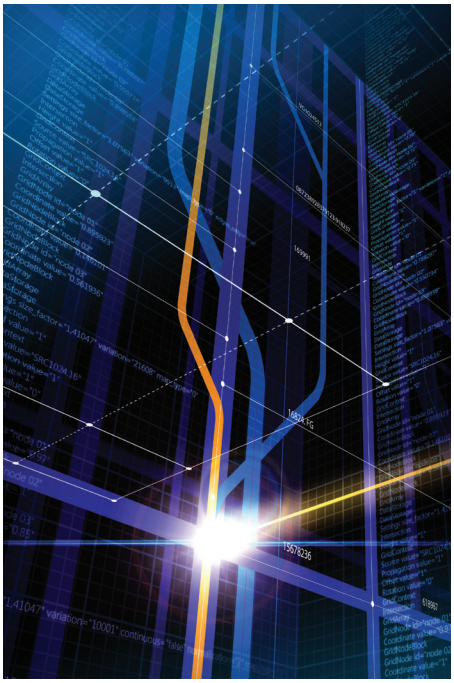
September 2015

EFT Data Management

Solving Wire Transfer and ACH Data Challenges

By Nikhil N. Fafat, Mohammad Nasar, and Christopher J. Sifter, PMP

Electronic funds transfers (EFTs) offer speed and convenience for bank customers as well as efficiency and low transaction costs for financial institutions. But the widespread use of wire transfers and automated clearinghouse (ACH) transactions also can present significant data management challenges, especially in terms of *Bank Secrecy Act* and anti-money laundering (BSA/AML) regulatory compliance.



Nonstandardized source data and complex data formatting structures can result in inaccurate, incomplete, or duplicate records that greatly complicate compliance efforts. These data issues also create additional encumbrances for line-of-business processes.

A proactive approach to EFT entity resolution (improving EFT data quality) can help financial institutions address these concerns, enabling more accurate alerts, more efficient investigations, and improved regulatory compliance.

Challenges of Working With EFT Data

The ability to accurately identify the various unique parties involved in a transaction is essential for compliance with BSA/AML regulatory requirements. This necessity applies not only to the financial institution's immediate customer but also to all counterparties (legal entities or a collection of entities that can pose a financial risk to the institution) to the transaction. A bank also must be able to identify links among the various counterparties and their accounts.

Because a bank's ability to meet these requirements can be complicated greatly by slight variations in customer names, addresses, and other identifying information, most existing BSA/AML software requires external tools and processing (such as in the data integration layer) to recognize and standardize common abbreviations and variations in order to cross-reference and aggregate information and to identify related transactions and accounts.

In addition to identifying unique and related parties, an AML system must be able to correctly identify the locations of transactions in order to accurately quantify the risk associated with a particular operation. Institutions also need to be able to identify and segment customers by risk profile – a university presents a significantly different AML risk from a casino, for example. Here again, the ability to accurately identify these customer segments depends on data quality and the consistent use of standardized formats.

These challenges are further complicated by the number of parties involved in each EFT transaction. Parties include the customer who initiates the transaction, the originating customer's bank, intermediary institutions such as the Federal Reserve Bank, the receiving bank, the recipient customer, and other corresponding institutions.

Adding even more stringent data collection requirements and more rigorous enforcement is almost certain to generate internal resistance.

Every time a new participant enters the transaction chain, new opportunities appear for errors and inconsistencies in data formatting. In fact, many data quality issues are beyond an individual institution's jurisdiction, since the initial data input often occurs at another institution.

Finally, it should be noted that the various institutions and interbank payment systems employ their own particular data file formats. These include the U.S. Federal Reserve Bank's Fedwire, the Clearing House Interbank Payments System (CHIPS) format for certain foreign exchange and euro-dollar transactions, the Society for Worldwide Interbank Financial Telecommunication (SWIFT) format for international wire transfers, and the NACHA format for domestic ACH transactions. This diversity among data formats adds further complexity to any data standardization effort.

Why Common Approaches Fall Short of What's Needed

Because most AML applications cannot inherently identify and coordinate duplicate entities, banks must resort to using a variety of other strategies to address EFT data issues. In a recent webinar for bank executives hosted by Crowe Horwath LLP, participants were asked to identify the techniques they use to address the challenges of working with EFT data. By far the most frequently named technique was stricter enforcement of the bank's data collection policies, a finding that seems consistent across the financial services industry.

Unfortunately, although stricter enforcement of data collection policies is the most widely used method for addressing EFT data quality issues, there are a number of drawbacks to this approach. For example, it is not at all uncommon for customer-facing personnel and managers in banks' primary lines of business to regard their banks' existing data collection and know-your-customer (KYC) requirements as being unnecessarily burdensome and intrusive. Adding even more stringent data collection requirements and more rigorous enforcement is almost certain to generate internal resistance.

An even greater drawback, however, is the inherently limited effectiveness of such an approach, which cannot be relied upon to produce significant improvement in data quality. The reason, as noted earlier, is that in most banks a sizable proportion of EFT transactions originate from outside the institution. Cracking down on inconsistent or nonstandardized data entry in the institution does nothing to address data collection problems generated elsewhere.

Other attempts to address data quality concerns are more technology-driven, yet these too generally achieve limited success. For example, developing a complex programming solution for standardizing data and aggregating related transactions is timely, expensive, and difficult to implement correctly. Such efforts generally require extensive internal IT expertise and resources.

Another common approach involves attempting to develop matching heuristics to eliminate duplication. The drawback of this technique is its tendency to generate multiple false positives, resulting in a significant increase in the volume of alerts that must be investigated. As a consequence, institutions often find that their compliance efforts actually become less efficient rather than more efficient.

EFT entity resolution must resolve ambiguities, duplication, and inconsistencies in identifying and aggregating related transactions and entities.

A More Effective Approach: EFT Entity Resolution

To avoid the shortcomings of the most commonly used efforts to improve EFT data quality, many banks are seeking a more effective approach that enables them to accomplish three fundamental steps:

1. Identify patterns of behavior (such as common originators and common beneficiaries).
2. Aggregate transactions that are tied to the same entity.
3. Aggregate alerts that are traced back to these entities.

A functional term that can be used to describe such a solution is EFT entity resolution. It must, in essence, resolve ambiguities, duplication, and inconsistencies in identifying and aggregating related transactions and entities, regardless of whether these ambiguities stem from nonstandardized data formatting or from varying, complex data file structures.

Contact Information

Nikhil Fafat is with Crowe Horwath LLP and can be reached at +1 312 899 4492 or nikhil.fafat@crowehorwath.com.

Mo Nasar is with Crowe and can be reached at +1 630 574 1846 or mo.nasar@crowehorwath.com.

Chris Sifter is a director with Crowe and can be reached at +1 312 857 7363 or chris.sifter@crowehorwath.com.

An effective EFT entity resolution approach that can overcome the limitations of the most commonly attempted solutions must function in all three major phases of EFT data processing:

1. **Data ingestion.** The system enters data from standardized raw formats and collects it in a central repository.
2. **Data resolution and cleansing.** The system standardizes and cleanses the data, merges similar entities, cross-references against master institution lists, and then links merged entities to their original transactions.
3. **Data delivery.** The system transforms and delivers data to match commonly used transaction monitoring systems such as NICE Actimize, Oracle® Mantas, and Fiserv Financial Crime Risk Management solutions.

In addition, an EFT entity resolution approach ideally will offer a number of other attributes. For example, an effective solution should include automated data inputs and outputs to reduce manual overhead and errors. It also should be scalable, allowing the institution to adapt to organic growth as well as merger and acquisition activity.

An effective EFT entity resolution approach also must be flexible enough to accommodate different methods of operation and transaction processes across various lines of business, and it should be capable of accommodating new data sources and operations that might be developed in the future.

The Goal: Proactive Data Management

In addition to improving BSA/AML compliance efforts, the ultimate goal of an effective EFT solution is to enable institutions to anticipate and adapt to future trends in transaction technology as well as future developments in regulatory requirements. With EFT transactions continuing to account for a growing share of bank transactions, such an approach can be a powerful tool for accelerating and empowering an institution's transaction monitoring and customer due diligence functions while simultaneously improving overall productivity and effectiveness.